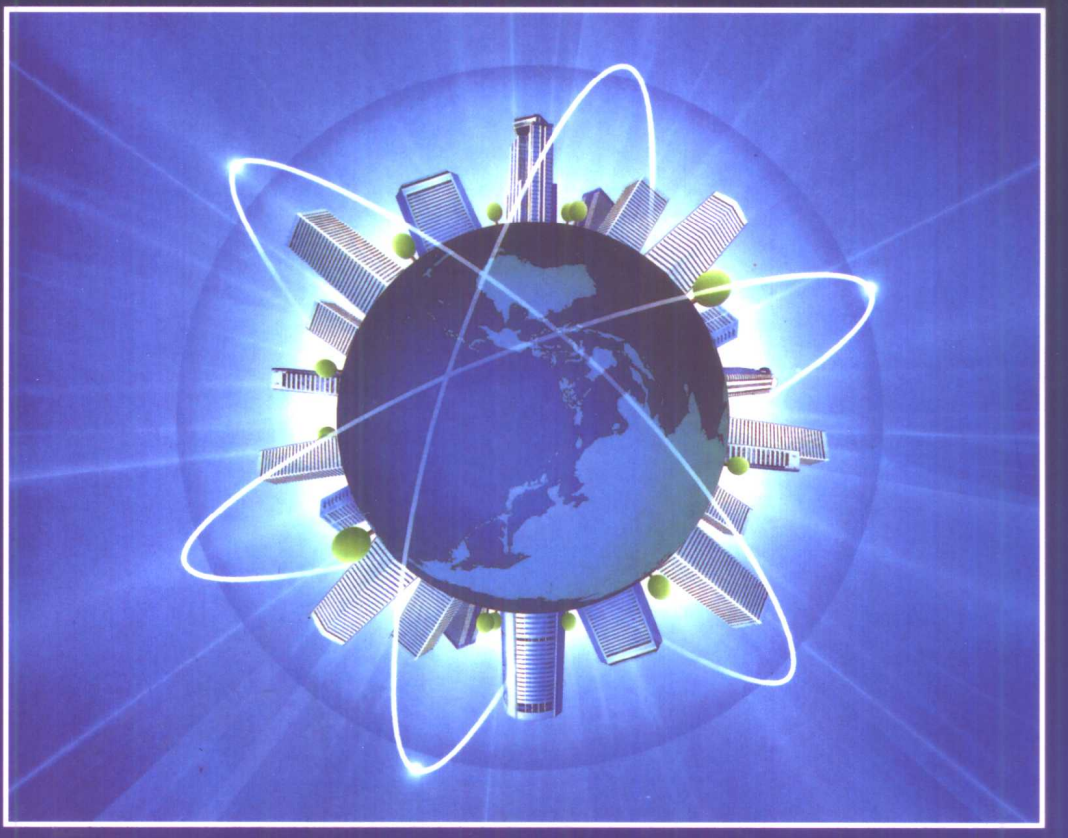
Internet Intranet

实用安全技术

张 超 编著



XDUP
西安电子科技大学出版社

Internet\Intranet 实用安全技术
张超 编著

Internet/Intranet
实用安全技术

张　超　编著

西安电子科技大学出版社

1999

内容简介

本书在分析 Internet 安全机制缺陷的基础上，以密码技术为核心，研究了常用的以及最新的网络安全技术，讨论了如何参照国际标准化组织(ISO)提出的网络安全体系结构这个概念模型来进行企、事业单位 Intranet 的安全性设计和建设。

本书既有理论又有实践，是目前较早系统全面介绍 Internet/Intranet 安全技术的书籍。

本书适用于从事网络设计、实施、管理的技术人员和从事信息化建设的有关人员使用，还可作为高等院校和科研机构专业人员的参考资料和培训教材。

Internet/Intranet 实用安全技术

张　超　编著

责任编辑　夏大平

出版发行　西安电子科技大学出版社

（西安市太白南路2号）

邮　编　710071

电　话　(029)8227828

经　销　新华书店

印　刷　空军电讯工程学院印刷厂印刷

版　次　1999年2月第1版

1999年2月第1次印刷

开　本　787毫米×1092毫米　1/16　印张 10.125

字　数　233千字

印　数　1～4 000 册

定　价　13.00元

ISBN 7-5606-0699-7/TP·0355

前　言

在以微电子、光电子、计算机、通信和信息服务业务为特征的信息时代，通信已成为人类社会进行传递信息、交流思想、传播知识的重要手段。随着人们对通信服务需求的日益增长和计算机与通信技术的紧密结合，单机网络化、局域网互联化(包括企事业团体建立的内部网——Intranet和将企业已有的局域网联入Internet)极为时尚。尤其是Intranet作为知识经济的基础和环境，更加引人关注。

由于Internet采用了开放性的体系结构，企事业团体一旦将自己的局域网联入Internet，就使一个封闭的系统变成了开放性的系统。同时，Intranet是Internet技术在企业内部网上的实现。因此，信息传输的广域性和网络协议的开放性使其面临比现在任何一种网络都更为严重的不安全问题，Internet上所使用的TCP/IP通信协议，其弱点是安全性差和网络管理机制弱。任何一个安全上的漏洞都会带来巨大的损失。

在Internet上已发生多次不安全事件。据美国FBI统计，每年因信息网络安全所造成的损失达75亿美元；美国金融时报报道，平均每20秒就发生一次入侵Internet计算机的事件；Internet上的防火墙1/3以上被突破；超过25%的企业报告其损失高于25万美元。

1994年，深圳市案犯甲某通过电脑网络登录到该市一家证券部的用户密码库，利用解密得到的用户密码进入某用户的空白帐户，在其上凭空增设可用资金110多万元，之后以每股5.45元的当日最高价买入10.32万股深宝A股，造成该种股票价格的剧烈波动。

1995年8月21日，美国华尔街日报报道，尽管金融界巨子——花旗银行装备了“防火墙”，并拥有其他高技术的防范措施，但还是被前苏联克格勃人员通过计算机网络盗窃了1 160万美元的巨资。

可笑的是，1996年12月31日美国《纽约时报》报道：“黑客更换网页，入侵空军金珠网”，黑客将空军网页修改为两只鲜血直流的红眼珠，并书写“欢迎了解真相”，对美国政府大肆攻击。美国司法部的互联网主页也曾被修改过。

Internet安全既涉及技术问题，也涉及到信息安全的管理机构与信息安全的策略、法律、技术、经济以及道德规范等。所谓网络安全，并非绝对安全，而是指一定程度上的网络安全，要根据实际需要和自身所具有的条件确定所需达到的安全程度。安全要求越高，系统所具备的安全功能就越多，其安全强度就越高，同时对网络的性能影响也越大。因为只有解决好网络的安全问题，才能

促进信息系统和网络运行的健康发展。

我国信息化建设处于起步阶段，网络安全管理机制也不健全，面临的网络安全问题极为严峻。据权威人士透露，目前我国的ChinaNet有80%的网络设备是美国Cisco公司的产品，网络的设计和实施也是由国外工程师完成的，更为严重的是整个网络没有国内产品进行监控约束，网络安全问题实在令网络工作者担心。正是出于这样一种责任感，迫使笔者孜孜不倦地消化吸收网络安全专家和学者们的研究成果并加以归纳，力求使网络安全技术理论化、系统化。同时，笔者认真总结网络安全性建设的经验，使本书具有实用参考价值，为我国信息化基础设施建设作出微薄的贡献。

本书以密码技术为主线来组织各个章节。首先从分析Internet安全机制的缺陷(在Internet上产生上述安全问题的主要原因)入手，来介绍一系列常用的和最新的网络安全技术。书的后部分讨论了国际标准化组织(ISO)提出的网络安全体系结构以及如何参照这个概念模型来进行企事业团体的Intranet的安全性设计和建设。书的结尾部分给出了一个实施网络安全性建设的案例。最后列举了部分常用的网络安全产品。

由于笔者的学识浅薄和时间仓促，书中难免有缺点和不足之处，有些观点和提法甚至是错误的，望读者不吝赐教。

在此，笔者衷心地感谢清华大学网络中心的黄峥嵘老师提供的珍贵资料，感谢西安电子科技大学夏大平老师的指导和热情帮助，还感谢网络安全专家和学者(见参考文献)对网络安全系统、信息系统所作的开创性研究。

编　　者

1998年元月2日于成都

目　录

第 1 章　网络操作系统和 TCP/IP 安全机制的缺陷

第 2 章　密 码 技 术

第 3 章　认 证 技 术

第 4 章　分布计算环境

第 5 章　操作系统的安全性

第 6 章　数据库系统安全技术

第 7 章　Web 安 全 技 术

第 8 章　ActiveX 及 Java 的安全性

第 9 章　防火墙技术

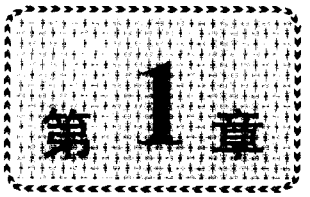
第 10 章　反病毒技术

第 11 章　安全管理技术

第 12 章　安全体系结构

第 13 章 安全产品及工具介绍

第 14 章 实施网络安全性建设案例



网络操作系统和TCP/IP安全机制的缺陷

UNIX、Windows NT 网络操作系统和 TCP/IP 通信协议虽然在 Internet/Intranet 上起着重要的作用，但它们在安全机制上却存在着不同程度的缺陷。

1.1 网络操作系统的缺陷

网络操作系统是计算机和用户之间的接口，是管理网络资源的核心系统，负责向通信设备发送信息，管理存储设备上的存储空间和将信息装入内存等调度工作。网络操作系统采用管理文件目录的方法进行管理，并且利用口令字标志存取控制权限，用加密及其它一些手段来提高文件的安全性。

在一个网络系统中，每个使用者均通过一个操作系统来出入网络，因此，操作系统的安全性对网络的安全性起着重要的作用。虽然有些人声称 UNIX、Windows NT 达到了 C2 标准，但实际上未完全真正实现。

1.1.1 UNIX 操作系统的缺陷

据统计，在传统的 UNIX 操作系统中有很多安全漏洞(已发现超过 100 个)。这些漏洞可以通过随操作系统附带的小的“Patches”(补钉)除掉。但这些小“Patches”只有在用户要求时厂商才予提供。实际上用户很少向厂商提出这一要求。

1. 特权用户权力过大

UNIX 的传统功能是通过特权系统来解决安全问题。这个特权系统中的特权由可信任的主管人来控制，并且文件的访问是通过文件允许比特(File Permission Bit)和访问控制列表(Access Control List)控制的。特权用户在系统安全体系中具有至高无上的权限，他可以更改系统中所有的数据，而对特权用户的保护仅是脆弱的口令保护。这是 UNIX 的一个致命的弱点。

2. 口令与帐户

UNIX 操作系统通常把加密的口令保存在一个静态的文件内，而普通用户即可读取该文件。这个口令文件可以通过简单的拷贝或其它方法得到，一旦口令文件被闯入者得到，

他们就可以使用解密程序。比如，Robert Morris 通过制造蠕虫(Worm)的方式来窃取文件。其方法是：Morris 通过一个名为 GUESSES 的程序来搜索 UNIX 的用户和相匹配的口令，这个程序在蠕虫开始传播的 4 天内就获得了 99 个口令，且这种效率呈几何量级升高，直至蠕虫感染了数以百计的 UNIX 服务器，打开了成千上万的文件。

安装 UNIX 时，有一些系统在缺省状态下，会自动建立一些帐户，比如 guset 等。由于这种帐户一般都有一个约定俗成的口令，因此如果您没有注意到它的存在，那么，任何人都可以随意地进入您的主机。与此相似，还有一种系统缺省建立的帐户，如 shutdown、sync。这种帐户一般是为了执行一个相关命令，所以是不设口令的。其 UID 多与 root 相同，因此具有与 root 同样的权限。一个黑客可以通过冒充这种帐户来取得 root 的权限。

3. 登录无次数限制

UNIX 在用户口令(Passwords)管理上相当薄弱，可称之为"有志者事'尽'成"，登录口令可以试无数次。假如口令的长度少于 8 个字符或是英语单词，就可能被破译，然后用来获取对系统的访问权。虽说 UNIX 的口令是通过一个单向函数生成的，但黑客们不是利用某种工具像求解逆函数那样把口令求解出来，而是利用口令猜测软件，经过长时间的组合能比较容易地猜测出口令。

4. 文件系统

在 UNIX 环境下存在着两种特殊的命令程序，即 Suid 和 Guid。它们的主要特点是：执行 Suid 程序的帐户会在本程序终止前拥有与该程序的所有者相同的 UID；与此类似，执行 Guid 程序的帐户会在本程序的终止前，拥有与该程序的所有者相同的 GID。因为在 UNIX 系统中，检查帐户权限的惟一根据就是该帐户的 UID 或 GID，所以这两种程序往往会成为黑客们极其感兴趣的目标。

1.1.2 Windows NT 的缺陷

Windows NT 的安全特点在于：安全登录设施；自由选定的访问控制，即资源的属主可以任意决定其他人的访问权限；审计、检测并有记录重要的与安全相关的事件；存储保护，防止任何人读出某人释放给操作系统在内存块中的信息。安全引用监控所起的作用就是保护系统的资源，执行的对象是保护和审计。Windows NT 虽然具备了相当强的单机安全性，但在分布式安全体系中，NT 的集中实体认证和数据加密功能则较弱。Windows NT 也不能限制对 Administer 帐号不成功登录的次数。

1.2 TCP/IP 的安全机制

1.2.1 TCP/IP 的发展

在 20 世纪 60 年代后期，人们开始认识到计算机和计算机网络互连的重要性，并开始研究这方面的问题。为了战争的需要，美国国防部要以分布方式连接大量的计算机，以方便相互之间的通信和资源共享。美国高级研究规划署 ARPA 为了实现不同类型网络的互

连，大力资助网络互连技术的研究，开发了各种软、硬件。在1969年，ARPA组建了Internet的前身ARPANET网，它的基本宗旨就是资源共享。

网络互连最基本的目的是在主机之间传送信息，因此，首先需要解决网络之间不相兼容的问题。网际协议IP是实现异种网络互连的关键。但网际协议所能提供的是不可靠的数据传输，可靠的数据传输是由传输控制协议TCP来保证的。为此。ARPANET的研究人员开发一系列的协议，这些协议通称为TCP/IP协议簇。这些协议采用的是分层协议互相配合，构成一个整体，完成不同的功能；且各层协议互相配合，构成一个整体，完成统一的功能。在TCP/IP推出不久，美国国防通信局于1983年要求所有连接在ARPA上的网络都要采用TCP/IP协议，从而也就导致了Internet的产生。

1.2.2 TCP/IP协议簇简介

TCP/IP是网络中使用的基本通信协议，虽然从名字上看TCP/IP包括两个协议，即传输控制协议(TCP)和网际协议(IP)，但TCP/IP实际上是一组协议，包括上百个互为关联的协议，最常用的几个协议是：

(1) Telnet(Remote Login)：提供远程登录功能，一台计算机用户可以登录到远程的另一台计算机上，如同在远程主机上直接操作一样；

(2) FTP(File Transfer Protocol)：远程文件传输协议，允许用户将远程主机上的文件拷贝到自己的计算机上；

(3) SMTP(Sample Mail Transfer Protocol)：简单邮政传输协议，用于传输电子邮件；

(4) NFS(Network File Server)：网络文件服务器，可使多台计算机透明地访问彼此的目录；

(5) UDP(User Datagram Protocol)：用户数据报协议，它和TCP一样位于传输层，和IP协议配合使用，在传输数据时省去包头，但它不能提供数据包的重传，所以适合传输较短的文件。

1.2.3 TCP/IP协议的数据传输原理

TCP/IP协议的基本传输单位是数据包(datagram)。TCP协议负责把数据分成若干个数据包，并给每个数据包加上包头(就像给一封信加上信封)；包头上有相应的编号，以保证在数据接收端能将数据还原为原来的格式；IP协议在每个包头上再加上接收端主机地址，这样数据就会找到自己要去的地方(就像信封上要写明地址一样)。如果传输过程中出现数据丢失、数据失真等情况，TCP协议会自动要求数据重新传输，并重新组包。总之，IP协议保证数据的传输，TCP协议保证数据的质量。

1.2.4 TCP/IP协议的层次结构

TCP/IP协议数据的传输基于TCP/IP协议的四层结构：应用层、传输层、网络层、链路层(接口层)。数据在传输中每通过一层就要在数据上加个包头，其中的数据供接收端同一层协议使用，而在接收端，每经过一层要把用过的包头去掉，这样来保证传输数据的格式完全一致。

TCP/IP协议簇中的协议分布在这四层结构中，如图1-1所示。

可见，TCP/IP 协议簇中的 TCP 协议位于传输层，IP 协议位于网络层。

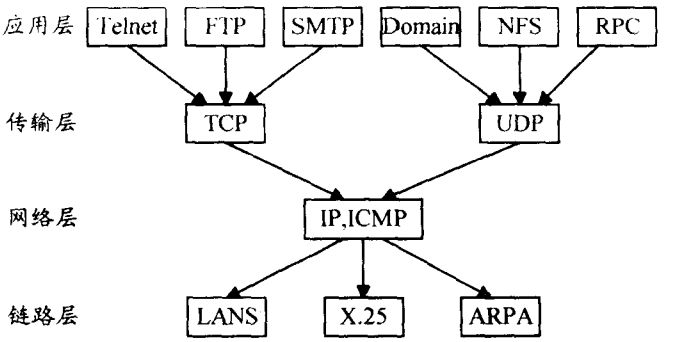


图 1－1　TCP/IP 协议簇四层结构

1.2.5　TCP/IP 的包头结构

TCP/IP 协议的基本传输单位是数据包。TCP 将上层应用传送(用户)的报文(较长的数据信息)划分成较小数据段，并在每个数据段加上 TCP 包控制头(其中包括宿主机地址，数据重构所需的信息和防止信息包被毁坏的信息)，从而形成了 TCP 包，其结构如表 1.1 所示。

表 1.1　TCP 的包头结构

信源端口号	信宿端口号
数据包序号	
应答包序号	
地址长度，最大缓冲区长度	
校验和	应急指针
用户数据	

在 TCP 包形成后，TCP 将它交给 IP，IP 将它作进一步的分解，并加上控制头(其中包括地址信息，以及装载的 TCP 信息和数据)，从而形成了 IP 包，其结构如表 1.2 所示。

表 1.2　IP 包头结构

IP 版本	地址长度	服务类型	数据包总长度(576 B～65 535 B)
识别码	标志		数据包相对偏移量
生存时间	协议		包头校验和
信源地址			
信宿地址			
TCP 包头信息			
用户数据			

1.2.6 TCP/IP协议簇的缺陷

在60年代，根据当时的技术和通信要求开发的TCP/IP协议，虽然获得了成功，但不能适应现代通信技术的需要，存在诸如IP地址空间不足，不能进行实时多媒体、音频传送以及电视点播等问题。本章仅讨论TCP/IP在安全方面的缺陷。目前已在TCP/IP上发现了100多种安全弱点或漏洞。

1. IP的缺陷导致易被欺骗

1）IP包中的源地址可以伪造

众所周知，IPv4的IP地址是可以用软件配置的，这就存在地址冒充和地址欺骗两个安全隐患。IPv4支持源路由方式，即显示规定信息传送的路径，也产生路由攻击隐患；Internet应用协议，如SMTP、Telnet、FTP等缺乏安全保密等措施。

指定路由发送方指定一信息包到达目的站点的路由，而这条路由是经过精心设计的、可绕过设有安全控制的路由。

假冒欺骗一般采用源IP地址欺骗攻击，入侵者伪装冒充源自一台内部主机的一个外部地点传送信息包。这些信息包中包含有内部系统的源IP地址。另外，在Email服务器，使用报文传输代理(MIA，Message Transfer Agent)，冒名他人，窃取信息。接收主机相信发送的主机(它说是谁就是谁)，邮件的来源就可以轻而易举地被欺骗，只需输入一个与真实地址不同的发送者地址，这就导致了任何没有特权的用户都可以伪造或欺骗电子邮件。

一个典型案件的原告与被告均为北京大学学生，原告于1996年4月9日收到美国密执安大学通过Internet发来的为其提供奖学金的电子邮件，但此后，她久等该大学的入学通知而无果。经调查，她认定在1996年4月12日上午10时16分，本案被告冒用她的名义又向密执安大学发去一封电子邮件，谎称其已接受其他学校的邀请，拒绝了密执安大学。被告在浏览原告电子邮件后，通过Internet使原告丧失入学资格。

2）IP包中的“生成时间”可以伪造

在TCP/IP网络中，由于发送者极易更改主机的系统时间，而接收主机又不作时间核实，它相信发送主机发送的时间(它说是什么时间就是什么时间)，这也容易导致伪造和欺骗。笔者曾尝试过，有一次同学发来Email，要求看后马上回Email，笔者却因种种原因忘了及时回Email，无奈间采用了一个骗术——把计算机时钟更改后再给同学回Email。这样一来，同学收到发回的Email虽晚，但Email上标识的生存时间却表明该Email早就发出。骗术果然奏效。

3）认证不可靠

在TCP/IP网络中把IP包中的信源/信宿地址作为许多服务的认证的基础，这样的认证是不可靠的。因为高层的TCP和UDP服务在接收数据包时通常是把IP包中的源地址看作是有效的，TCP和UDP服务相信数据包是从一个有效的主机发送来的。IP确实包含一个选项(即IP source routing)，可以用来指定一条源地址和目的地址之间的直接路径。这条路径可以包括通常不被用来向前传送包的主机或路由器。对于一些TCP和UDP的服务来说，使用了该选项的IP包好像是从路径上的最后一个系统来的，而不是来自它的真实地点。这个选项是为了测试而存在的，然而说明了它可以被用来欺骗系统以进行平常不被允许的连接。那么，许多依靠IP源地址确认的服务就会产生问题并且会被非法进入。

下面的例子说明了如何使用这个选项来把攻击者的系统假扮成某一特定服务器的可信任的客户。

(1) 攻击者要使用那个被信任的客户的地址取代自己的地址；

(2) 攻击者构成一条要攻击的服务器和其主机间的直接路径，把被信任的客户作为通向服务器的路径的最后节点；

(3) 攻击者用这条路径向服务器发出客户申请；

(4) 服务器接收客户申请，就好像是从可信任客户直接发出的一样，然后给可信任客户返回响应；

(5) 可信任客户使用这条路径将包向前传送给攻击者的主机。

许多 UNIX 主机接收到这种包后将继续把它们向指定的地方传送。一个更简单的方法是攻击者等客户系统关机后来模仿该系统。许多组织中，UNIX 主机作为局域网服务器使用，职员用个人计算机和 TCP/IP 网络软件来连接并使用它们。个人计算机一般使用 NFS 来对服务器的目录和文件进行访问(由于 NFS 仅仅使用 IP 地址来验证客户)。一个攻击者几小时就可以设置好一台与别人名字和 IP 地址相同的个人计算机，然后与 UNIX 主机建立连接，伪装成真正的客户。这是极易实行的攻击手段。

2. ICMP 的缺陷

ICMP 中的“Redirect”消息可以用来欺骗主机和路由器，使它们使用“假”路径。这些假路径可以直接通向攻击者的系统而不是一个合法的可信赖的系统。这会使攻击者获得系统的访问权。

对于系统来说，缺乏反映信源到信宿真实路径的跟踪信息。通过 TCP/IP 发出一个数据包如同把一封信丢入信箱，发出者知道正在走向信宿，但发出者不知道通过什么路线或何时到达。这种不确定性也是安全漏洞。

3. TCP 和 UDP 端口结构的缺陷

TCP 和 UDP 服务通常有一个客户/服务器的关系。例如，一个 Telnet 服务进程开始在系统上处于空闲状态，等待着连接。用户使用 Telnet 客户程序与服务进程建立一个连接。客户程序向服务进程写入信息，服务进程读出信息并发回响应。客户程序读出响应并向用户报告。因而，这个连接是双工的，可以用来进行读写。

两个系统间的多重 Telnet 连接是这样相互确认并协调一致的，即 TCP 或 UDP 连接惟一地使用每个消息中的如下四项进行确认：

(1) 源 IP 地址——发送包的 IP 地址；

(2) 目的 IP 地址——接收包的 IP 地址；

(3) 源端口——源系统上的连接的端口；

(4) 目的端口——目的系统上的连接的端口。

端口是一个软件结构，被客户程序或服务进程用来发送和接收消息。一个端口对应于一个 16 bit 的数。1 024 个端口号已分配给专门的服务，用户的应用程序可使用的端口号为 1 024 到 64 000。即服务进程通常使用一个固定的端口，例如：

FTP：	使用 21	Telnet：	使用 23
SMTP：	使用 25	Login：	使用 49

Domina：	使用 53	Finger：	使用 79
HTTP：	使用 80	Hostname：	使用 101
Who：	使用 513	UUCP：	使用 540
X - Windows：	使用 6 000		

这些端口号是“广为人知”的，因为在建立与特定的主机或服务的连接时，需要这些地址和端口号。这为攻击者提供了公开的秘密。

4. TCP/IP 明码传送信息导致易被监视

在网络中最常见的窃听是发生在共享介质的网络中，如 Ethernet(以太网)，这是由于 TCP/IP 网络中众多的网络服务均在网络中明码传送，而众多的网络使用者觉察不到。大多数的“黑客”(Hacker)均使用 Sniffer、Tcpdump 或 Snoop 等探测工具，可以清楚地看到某个用户从一台机器登录到另一台机器的全过程。

应该注意到，当用户使用 Telnet 或 FTP 连接到远程主机上时，他在 Internet 上传输的口令是没有加密的。侵入系统的另一个方法，就是通过监视携带用户名和口令的 IP 包获取它们，然后使用这些用户名和口令，通过正常渠道登录到系统。如果被截获的是管理员的口令，那么获取特权级访问就变得更加容易。就像前面曾说过的，成百的或数千的系统已经被这种方法侵入。

X - Windows 系统是一个逐渐流行起来的系统，但它同样也存在易被监视的弱点。X - Windows 系统允许在一台工作站上打开多重窗口来显示图形或多媒体应用。闯入者有时可以在另外的系统上打开窗口来读取可能含有口令或其它敏感信息的击键序列。

5. 提供不安全的服务

1) 匿名服务 FTP

未经授权的用户可以通过简单接入 TCP/IP，作为一个匿名的用户存取文件，而不正确的配置将严重威胁系统的安全。黑客可以在一个具有写权限的目录内安置一个“特洛依木马”，并能相当容易地捕捉口令和进入各子网。

TFTP 也是个相当危险的文件传输服务，由于它根本不作登录与控制审查，任何人都可以通过它取走您的具有读权限的文件。

2) Finger

在 TCP/IP 协议中，只需一个 IP 地址便可以提供许多关于主机的信息，比如谁正在登录、登录时间、地点，等等。对一个训练有素的黑客来讲，Finger 无疑是其进入目标主机的一把利器。因为知道了用户名就等于成功了一半。

3) 受托访问

在大型的网络环境下，受托访问可以为用户带来很多方便。但在方便的背后，潜藏着又一个安全隐患。从受托访问的过程可以看出，如果黑客偶然得到了您的/etc/. hosts. equiv 文件，那么他就可以以一个合法的用户名用 Rlogin 进入您的主机。

4) 不安全的网络服务

在 TCP/IP 中，echo、systat、netstat、bootp、udp、tftp、link、supdup、sunprc、news、snmp、xdmcp、exec、login、shell、printer、biff、who，syslog、uucp、route、openwin、NFS、X11 等服务被认为是不安全的，尤其是那些依赖于入呼叫包的 UDP 的服务。由于 UDP 无

需建立初始化连接(握手)，亦即两个主机系统之间没有虚电路(Virtual Circuit)，与 UDP 相关的服务面临着更大的危险。

5) NFS

NFS 的功能是安装跨网文件系统。对终端用户来说，它在本地和远地文件系统之间可以建立透明连接。有些版本的 NFS 系统的这个进程具有向安装进程转发安装请求的功能：一个黑客可以获得对一个错误配置的 NFS 服务器的非授权存取，因为安装进程会像处理直接从 Portmap 发来的请求那样对这种转发请求进行处理。

1.3 小　　结

目前所使用的网络操作系统，由于在系统结构设计和代码设计时偏重于考虑系统的使用方便性，至于安全性则很少顾及，导致系统的安全机制不健全(如权限管理，口令管理等)，存在许多安全漏洞，给攻击者以可乘之机。即使现阶段采用“Patches”手段，但仍然解决不了根本性问题。

目前在 Internet 上使用的 TCP/IP 协议，是出自建立 ARPANET 而开发的一个协议簇，其初衷是通过把各种异种机联结起来以建立一个资源共享的网络——谁想用谁就用的自由网络。它强调了系统的开放性，忽略了系统的安全性。因此，TCP/IP 协议潜在着严重的安全隐患，包括提供的网络服务。